IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
(Attorney Docket № 15415US01)

In the Application of:

    Sherman Chen, et al.

Serial No. 10/769,173

Filed: January 30, 2004

For: A SECURE KEY AUTHENTICATION
       AND LADDER SYSTEM

Examiner: Yogesh Paliwal

Group Art Unit: 2435

Confirmation No. 7811

Electronically filed on 08-SEP-2009

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

    The Applicant requests review of the final rejection in the above-identified application, stated in the final Office Action mailed on June 10, 2009 ("Final Office Action") with a period of reply through September 10, 2009. No amendments are being filed with this request.

    This request is being filed with a Notice of Appeal. The review is being requested for the reasons stated on the attached sheets.

REMARKS

The present application includes pending claims 1-41, all of which have been rejected. Claims 1-41 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Akiyama, U.S. Pub. No. 2002/0001386 (hereinafter, "Akiyama"), in view of U.S. Patent No. 6,073,237 (hereinafter, "Ellison"). The Applicant respectfully submits that the claims define patentable subject matter. The Applicant also respectfully traverses these rejections at least for the following reasons:

I. The Proposed Combination of Akiyama and Ellison Does Not Render Claims 1-41 Unpatentable

The Applicant now turns to the rejection of claims 1-41 as being unpatentable over Akiyama in view of Ellison. The Applicant notes that the proposed combination of Akiyama and Ellison forms the basis for all of the pending rejections.

A. Independent Claims 1, 11, 21, and 32

With regard to the rejection of independent claim 1 under 103(a), the Applicant submits that the combination of Akiyama and Ellison does not disclose or suggest at least the limitation of "encrypting the digitally signed secure key utilizing at least a previously generated unreadable digitally signed and encrypted secure key, **wherein said previously generated unreadable digitally signed and encrypted secure key was generated by encrypting a previously generated digitally signed secure key**," as recited by the Applicant in independent claim 1.

The Examiner concedes the following in page 7 of the Final Office Action:

> Akiyama does not disclose that the master key is also encrypted and digitally signed and wherein said previously generated unreadable digitally signed and encrypted key (master key) was generated by encrypting a previously generated digitally signed secure key (master key) as now required by claim limitation.

The Examiner has, in effect, conceded that Akiyama does not disclose the above stated limitation from Applicant's claim 1. The Examiner then relies for support on Ellison and states the following:

> Ellison, in the same field of endeavor of network security, discloses encrypting and digitally signing a key wherein encryption of the key takes place after digitally signing the key (Column 4, lines 64-67, **"The session key Kx is signed by private key of the server itself Kn 121 and encrypted by the public key of the user P1e**. The encrypted and signed session key Kx is then sent back to the user 123, further note that since the encryption of session key Kx is taking place before the encryption, it reads on to the amended claim limitation that requires key to be encrypted and digitally signed wherein the digitally signed and encrypted key was generated by encrypting a digitally signed key).

See Final Office Action at pages 7-8. Since Ellison uses the public key P1e to encrypt the session key, then it is Ellison's public key P1e that is being equated to Applicant's "at least a previously generated unreadable digitally signed and encrypted secure key". The Applicant respectfully disagrees that Ellison overcomes the above deficiency of Akiyama at least based on two reasons.

Firstly, the Applicant recites an unreadable, as well as signed and encrypted, secure key. Obviously, Ellison's public key P1e is neither unreadable (it is known that the public key in PKI encryption systems is communicated to many users), nor it is signed or encrypted.

Secondly, the Applicant specifically recites how the "previously generated unreadable digitally signed and encrypted secure key" is generated. More specifically, the previously generated unreadable digitally signed and encrypted secure key is generated "by encrypting a previously generated digitally signed secure key." Again, Ellison does not provide any disclosure as to how the public key is generated.

Therefore, Ellison does not overcome the above deficiencies of Akiyama, which were conceded in the Final Office Action, and claims 1, 11, 21, and 32 are allowable. The Applicant also maintains all arguments stated in pages 12-22 of the August 10, 2009 response.

II.   Conclusion

The Applicant respectfully submits that claims 1-41 of the present application should be in condition for allowance at least for the reasons discussed above and request that the outstanding rejections be reconsidered and withdrawn. The Commissioner is authorized to charge any necessary fees or credit any overpayment to the Deposit Account of McAndrews, Held & Malloy, Ltd., Account No. 13-0017.

Respectfully submitted,

Date: __08-SEP-2009__   By: __/Ognyan I. Beremski/_____

                                                Ognyan Beremski, Reg. No. 51,458
                                                Attorney for Applicant

McANDREWS, HELD & MALLOY, LTD.
500 West Madison Street, 34th Floor
Chicago, Illinois 60661
Telephone: (312) 775-8000
Facsimile: (312) 775-8100
(OIB)